AFFIDAVIT OF JOSHUA BEN MAYERS
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

SEALED

I, Joshua Ben Mayers, being sworn, state:

1. I have been a Special Agent for the Federal Bureau of Investigation (FBI) for the past 21 years. I am currently assigned to the Madison Resident Agency. I have been the affiant for many complaint and search warrant affidavits, have made numerous arrests, and have executed many search warrants.

2. I have participated in this investigation, reviewed the forensic results of some of the searches described below, and discussed the case with other law enforcement officers, business executives and employees of the victim company, American Superconductor (AMSC) a United States-domiciled company that produces software and hardware for the wind energy industry. I believe that the law enforcement officers, the business executives, and victim company employees are all credible because their information has been corroborated by: (a) information stored within the Massachusetts wind turbines described below; (b) the forensic examination of electronic media discussed below; and (c) emails between persons who are other targets of this investigation recovered through search warrants issued by this Court. I have also reviewed a comprehensive report prepared by a multinational consulting corporation that acted, in this case, as private corporate fraud investigators. I believe the facts related in the comprehensive report to be reliable for the same reasons I trust the facts related to me by the representatives of AMSC. Based on this information and on my training and experience, I am providing the following information in support of

the attached complaint. This complaint affidavit does not reflect the entirety of the investigation, but rather, I am focusing on those facts relating to the proposed charges against Dejan Karabasevic (Karabasevic).

3. The Federal Bureau of Investigation and the United States Attorney's Office for the Western District of Wisconsin are investigating Karabasevic, a wind turbine manufacturer located in the People's Republic of China (hereafter, the Company), two employees of the Company, identified here as Individual A and Individual B, and others associated with the Company, for numerous crimes, including those alleged in the complaint: (1) conspiracy, under Title 18, United States Code, Section 371, to commit felony copyright infringement in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Section 2319; and (2) unauthorized access to a Middleton, Wisconsin, computer to obtain information with a value of more than $5,000 and where the offense was committed for commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C). In sum, the facts described herein show:

(a) Beginning in approximately 2007, the Company had a business relationship with AMSC and purchased software and hardware from AMSC for use in wind turbines manufactured in China;

(b) The Company recruited Karabasevic, an employee of an AMSC subsidiary located in Austria;

(c) Karabasevic unlawfully downloaded the copyright-protected source code

for particular software from an AMSC computer located in a subsidiary AMSC office in Middleton, Wisconsin computer that was connected to the AMSC computer network;

(d) Karabasevic modified the source code and then provided a modified version of AMSC's software to the Company, thus eliminating the Company's need to purchase or license the software generated from the source code from AMSC; and

(e) The Company then used the copyright-protected software provided to them by Karabasevic on more than ten wind turbines without paying AMSC.

The Facts

4. AMSC's corporate headquarters is in Devens, Massachusetts, with additional United States offices in Middleton and New Berlin, Wisconsin. According to William Vareka, a senior software manager for AMSC, in March 2011, AMSC stored a certain category of "source code" on a computer in the Middleton, Wisconsin office in the Western District of Wisconsin. The Middleton computer acted as a "server" within the AMSC computer network as it was dedicated in part to hosting and storing source code folders. In this context, source code is a set of high-level computer commands that, once it is finalized, is "compiled" into computer-useable software. Vareka explained that the compiler is a computer program that transforms source code written in a programming language to binary code which can be used on a computer to

perform the functions as directed by the software compiled from the source code.

5. Among other things, AMSC produces equipment and software that regulate the flow of electrical energy from wind turbines to electrical grids. One AMSC product is software compiled from the source code stored in Middleton, Wisconsin. This particular source code is identified as source code version 5650414_R1. The Company initially contracted to purchase software compiled from source code version 5650414_R1 for two reasons: (1) to retrofit a large number of existing wind turbines in China to comply with revised electrical grid requirements; and (2) to make newly-manufactured turbines safer and more efficient. The source code version 5650414_R1 and the software compiled therefrom are copyright-protected intellectual property of AMSC. Vareka explained that source code version 5650414_R1 was created in Wisconsin and was stored on a computer in the AMSC Middleton, Wisconsin office. Vareka explained that source code version 5650414_R1 was finalized on February 1, 2011. Vareka further explained that an additional AMSC proprietary software program, identified as the "checksum generator," was also stored in the Middleton, Wisconsin computer and that the "checksum generator" was necessary to run software compiled from source code version 5650414_R1. The "checksum generator" is a critical software tool created by AMSC. This software tool is used, among other things, to make the compiled source code version 5650414_R1 operational. Without the "checksum generator," Karabasevic could not have given the Company an operational version of the software that he compiled from source code version 5650414_R1. Both

perform the functions as directed by the software compiled from the source code.

5. Among other things, AMSC produces equipment and software that regulate the flow of electrical energy from wind turbines to electrical grids. One AMSC product is software compiled from the source code stored in Middleton, Wisconsin. This particular source code is identified as source code version 5650414_R1. The Company initially contracted to purchase software compiled from source code version 5650414_R1 for two reasons: (1) to retrofit a large number of existing wind turbines in China to comply with revised electrical grid requirements; and (2) to make newly-manufactured turbines safer and more efficient. The source code version 5650414_R1 and the software compiled therefrom are copyright-protected intellectual property of AMSC. Vareka explained that source code version 5650414_R1 was created in Wisconsin and was stored on a computer in the AMSC Middleton, Wisconsin office. Vareka explained that source code version 5650414_R1 was finalized on February 1, 2011. Vareka further explained that an additional AMSC proprietary software program, identified as the "checksum generator," was also stored in the Middleton, Wisconsin computer and that the "checksum generator" was necessary to run software compiled from source code version 5650414_R1. The "checksum generator" is a critical software tool created by AMSC. This software tool is used, among other things, to make the compiled source code version 5650414_R1 operational. Without the "checksum generator," Karabasevic could not have given the Company an operational version of the software that he compiled from source code version 5650414_R1. Both

computer source code version 5650414_R1 and the "checksum generator" program were original works of authorship, belonging to AMSC, that were fixed in a tangible medium of expression,[1] namely, the folder stored on an AMSC computer server in Middleton, Wisconsin. AMSC incorporated the term "copyright" into source code version 5650414_R1 and took deliberate steps to protect source code version 5650414_R1, the "checksum generator" program, and its other intellectual property from unauthorized use. John W. Powell, AMSC Vice President and General Counsel, stated that the value of source code version 5650414_R1 greatly exceeds $5,000 and that millions of dollars were invested in the development of this source code.

6. Daniel P. McGahn, AMSC President and Chief Executive Officer, John W. Powell, AMSC Vice President and General Counsel, and AMSC Attorney John Samia provided the information in paragraphs 6 through 8. Dejan Karabasevic (Karabasevic), was employed by AMSC Windtec GmbH (AMSC Windtec), in Klagenfurt, Austria. Karabasevic started with Windtec as a development engineer in 2004. In 2007, AMSC acquired Windtec which was then renamed AMSC Windtec. Karabasevic was eventually promoted to head of the Automation Engineering Department at AMSC Windtec. As an AMSC employee, Karabasevic certified his understanding, most recently on March 31, 2010, of AMSC's Code of Business Conduct and Ethics. That code required Karabasevic: to act in the best interests of AMSC; to avoid conflicts of interest;

---

[1] A "copyright" is defined by two requirements, originality and fixation: a work must be an original, creative expression of an idea or concept, and it must be recorded in tangible form. 17 U.S.C. § 102(a).

to not disclose confidential business information; to protect AMSC assets; and to not use AMSC assets for his or another's personal gain. In addition, Karabasevic acknowledged the AMSC Information Technology Policies on May 17, 2010. One of those policies prohibited use of the AMSC computer network to violate AMSC standards of ethics or to transmit proprietary information in any manner inconsistent with AMSC policies and directives. Karabasevic was not authorized to access AMSC computers to download its source code or other intellectual property, including but not limited to, the source code version 5650414_R1, nor was he authorized to distribute it to others.

7. Karabasevic's job required him to travel to China approximately ten times per year to support AMSC software and hardware. Karabasevic's work in China put him in frequent contact with employees and representatives of the Company, which in March 2011, represented nearly 80 percent of AMSC's business. On March 10, 2011, Karabasevic resigned from AMSC Windtec. The resignation was accepted the following day. Karabasevic retained access to the AMSC Windtec office in Klagenfurt, Austria, and to the AMSC computer system, into June 2011.

8. In late March 2011, the Company abruptly stopped paying for shipments from AMSC. Consequently, AMSC lost substantial revenue and was forced to lay off nearly half of its work force. As AMSC's revenues fell, its market value dropped from approximately $1.6 billion to approximately $200 million.

9. The comprehensive report prepared by the multinational consulting company, acting in this matter as private investigators (hereafter private investigators),

indicates that in June 2011, AMSC China employees, while conducting field work on behalf of AMSC, discovered operational, unauthorized versions of the AMSC software believed to be compiled from source code version 5650414_R1 in use within the Company's turbines at a wind farm in China. The unauthorized versions of AMSC software contained functionality that AMSC had not released to the Company. AMSC had only released a test version of the software compiled from source code version 5650414_R1 that was only designed to work for 14 days. The versions running on the Chinese wind farm were working well after the two-week test period had expired. The AMSC China employees copied and sent the unauthorized versions to AMSC Windtec, Klagenfurt, Austria. Examination of the unauthorized versions by AMSC employees indicated that the Company was using an unauthorized version of the software compiled from source code version 5650414_R1. The AMSC employees further concluded that the changes could not have been made without access to the source code folder stored only on a computer at the AMSC office in Middleton, Wisconsin. AMSC officials suspected that Karabasevic had provided the unauthorized source code to the Company.

10. Emails found within Karabasevic's computers obtained from his Beijing and Klagenfurt, Austria apartments--the physical and forensic searches of which are described below--as well as documents found in Karabasevic's Beijing apartment, showed that between approximately September 2010 and February 2011, Karabasevic negotiated an employment contract with the Company. Karabasevic and the Company

agreed to a six-year contact beginning in May 2011, with Karabasevic's total compensation exceeding 11 million renminbi, which equates to approximately $1.7 million U.S. dollars. Emails described below also show that Karabasevic had provided the latest version of the software compiled from source code version 5650414_R1 to the Company and that he had adapted AMSC source code so that it would function in the Company's turbines without license or authorization from AMSC.

11. In July 2011, Karabasevic gave written permission, in the presence of a representative of Dorda Brugger Jordis (DBJ), an Austrian law firm, to search the Beijing apartment that the Company had provided for him. On July 9, 2011, private detectives searched Karabasevic's Beijing apartment, finding two laptop computers, an external hard drive, and documents. Included within the documents were employment contracts negotiated between Karabasevic and the Company. The six-year contract between Karabasevic and the Company began on July 1, 2011 and would have paid Karabasevic more than 11 million renminbi (approximately $1.7 million U.S. dollars). The investigators also found a separate, one-year "service contract" requiring Karabasevic to work for a Chinese wind turbine blade manufacturer from July 1, 2011 through June 30, 2012. Based on my knowledge of this case, I believe that the separate "service" contract was a ruse to cover the fact that Karabasevic was really working for the Company.

12. The next day, July 10, 2011, at the Vienna, Austria airport, an AMSC China employee turned over the evidence obtained from Karabasevic's Beijing apartment to a

representative of the private investigative firm. Subsequently, the Beijing evidence was turned over to Austrian law enforcement authorities through DBJ, the Austrian law firm. Around the same period, Austrian law enforcement officers secured computers and other electronic storage media from Karabasevic's Klagenfurt, Austria apartment. Forensic copies of the computers and electronic storage media obtained from Karabasevic's Beijing and Klagenfurt apartments were analyzed by forensic analysts working with the private investigative firm referenced above. The forensic examination of the computers and electronic storage media found in Karabasevic's Beijing and Klagenfurt apartments showed that he had stored, possessed, and manipulated AMSC proprietary data on the computers and electronic storage media. In particular, the entire folder containing source code version 5650414_R1 and the "checksum generator" program downloaded on March 7, 2011, from the AMSC Middleton, Wisconsin, computer were found on a laptop computer found in Karabasevic's Beijing apartment. The analysis further showed, consistent with Karabasevic's confession described herein, that the information downloaded from AMSC Middleton, Wisconsin, had been adapted for use with equipment associated with the Company's wind turbines.

Charlestown, Massachusetts Turbine

13. The alleged theft of intellectual property under investigation led to litigation between AMSC and the Company and to significant publicity. Sumul Shah, Chief Operating Officer of Solaya Energy, LLC., and President of Lumus Construction, Wilmington, Massachusetts, learned of the potential theft of intellectual property and

invited AMSC to inspect a turbine manufactured by the Company that Lumus was installing at 172 Alford Street, Charlestown, Massachusetts. Shah told me that Lumus was installing the turbine for the Massachusetts Water Resources Authority and that Lumus had a contract to maintain the turbine after installation.

14. On March 22, 2012, the Honorable Magistrate Judge Jennifer C. Boal, District of Massachusetts, signed a warrant to search the Charlestown turbine for, among other things, digital evidence of the stolen/modified AMSC code. (12-MJ-7044-JCB). On March 28, 2012, the FBI executed the search warrant and seized digital evidence from the Charlestown turbine.

Scituate, Massachusetts Turbine

15. On May 10, 2012, Sumul Shah gave consent to search a different turbine manufactured by the Company which was located in Scituate, Massachusetts, along with an adjacent storage container. FBI agents searched the Scituate turbine on May 15, 2012, and copied information from equipment in the turbine.

Forensic analysis

16. In consultation with AMSC engineers, Special Agent Matt Petersen, FBI, reviewed three categories of electronic evidence: (a) Karabasevic's computers and electronic storage media seized from his Beijing and Klagenfurt apartments; (b) the software code Karabasevic emailed to his contacts at the Company; and (c) the information downloaded from the Charlestown and Scituate turbines. In summary, Petersen's analysis shows:

(a) Karabasevic downloaded the source code version 5650414_R1 and the "checksum generator" from Middleton on or about March 7, 2011;

(b) Karabasevic transferred source code version 5650414_R1 and the "checksum generator" program to other devices including a Lenovo laptop;

(c) A modified version of source code version 5650414_R1 exists on the Lenovo laptop. There were three minimal modifications to the source code. The changes, while minimal, allowed the Company to use the software without limitation.

(d) A version of the modified and compiled software compiled from the source code version 5650414_R1 exists on the Lenovo laptop. The "checksum generator" was applied to the modified software in order for it to function. Karabasevic sent portions of the modified and compiled version of this software to Individual A on at least May 28, 2011 and June 11, 2011.

17. Senior AMSC Software Manager William Vareka conducted extensive analysis comparing the authorized AMSC software generated from source code version 5650414_R1 with the unauthorized versions of the software resulting from Karabasevic's unauthorized downloading, modifying, and compiling source code version 5650414_R1 that were found within: the June 11, 2011 email Karabasevic sent to Individual A and the wind turbines manufactured by the Company located in Charlestown and Scituate, Massachusetts. Based on his analysis, Vareka determined that the software attached to the June 11, 2011 email Karabasevic sent to Individual A

and found in the wind turbines manufactured by the Company located in Charlestown and Scituate, Massachusetts, were all generated from source code version 5650414_R1.

Electronic Communications Involving Karabasevic and Individuals A and B

18. Written Skype "chat" conversations were found within Karabasevic's computers obtained from his Beijing and Klagenfurt, Austria apartments--the searches of which are described above. Skype "chat" communications between Karabasevic and Individual B indicate that the Company had begun to copy the unauthorized software compiled from source code version 5650414_R1 as early as June 2, 2011. In addition, Karabasevic used a Google e-mail account, dejan.karabasevic@gmail.com, to communicate with Sinovel employees regarding his employment with Sinovel, and to provide the stolen/modified AMSC code discussed above. Karabasevic communicated electronically with at least two employees of the Company, Individual A and Individual B. Individual A worked as a Deputy Director for Research and Development for the Company. Individual B worked as a Technology Manager for the Company. Individual A used a number of e-mail addresses, including a Google e-mail account to communicate with Karabasevic. Individual B used a Yahoo! e-mail account to communicate with Karabasevic.

19. Karabasevic exchanged well-over 200 e-mails with Individual B's Yahoo! e-mail account and Individual A's Google e-mail account. Karabasevic also used his Google e-mail account to provide modified software compiled from the source code version 5650414_R1 to Individual A on at least two occasions, May 28, 2011 and June 11,

2011.

20. Individual A used Individual A's Google account to notify Karabasevic of error messages Individual A received after testing the stolen and modified AMSC code on wind turbines in China. Using his Google e-mail account, Karabasevic sent modified AMSC code to Individual A and sent directions to other employees of the Company as he helped them to implement the software compiled from source code version 5650414_R1 and other intellectual property that Karabasevic stole from AMSC.

21. Search warrants issued by this Court and executed on the Yahoo! and Google email accounts used by Individuals A and B resulted in the recovery of thousands of emails in Chinese. Preliminary translations indicate that many Company employees--including Individuals A and B--used Google and Yahoo! to conduct business on behalf of the Company. The earliest emails recovered are contemporaneous with Karabasevic's work for the Company in China during June 2011. The latest emails were sent in April 2012. The preliminary translations indicate that many emails concern implementing the stolen software on turbines in China and on exported turbines. For example, a December 6, 2011, spreadsheet attached to an email suggests that more than 400 wind turbines in a particular area in China had been retrofitted with the unauthorized software compiled from source code version 5650414_R1. In an email dated December 29, 2011, an employee of the Company advises his colleagues--including Individual B--not to export turbines with software pre-loaded, but rather, to wait until the turbines are commissioned in the country to which the turbine had been

exported. I believe that this direction is intended to avoid inspection by import authorities. Emails obtained through the search warrant process also indicate that Individual B was the Company's project manager for installing turbines manufactured by the Company in Charlestown and Scituate, Massachusetts.

Sworn to under the penalties of perjury.

Joshua Ben Mayers
Special Agent, Federal Bureau of Investigation

Sworn to and subscribed before me this 5th day of November, 2012.

STEPHEN L. CROCKER
United States Magistrate Judge